Edición 21 - Abril 2026

Ciber E-dea

Revista de Ciberseguridad

e-dea NETWORKS | CYBER SECURITY

Great Place To Work. Certificada

icontec ISO 9001 CO-SC-CER893598

icontec ISO 45001 CO-ST-CER690599

icontec ISO / IEC 27001 CO-SI-20001007

IQNET

01 108 extensiones maliciosas de Chrome roban datos de Google y Telegram

02 Expertos alertan: violación del sistema de vigilancia del FBI es un incidente grave

03 Adobe corrige una vulnerabilidad de Acrobat Reader (CVE-2026-34621)

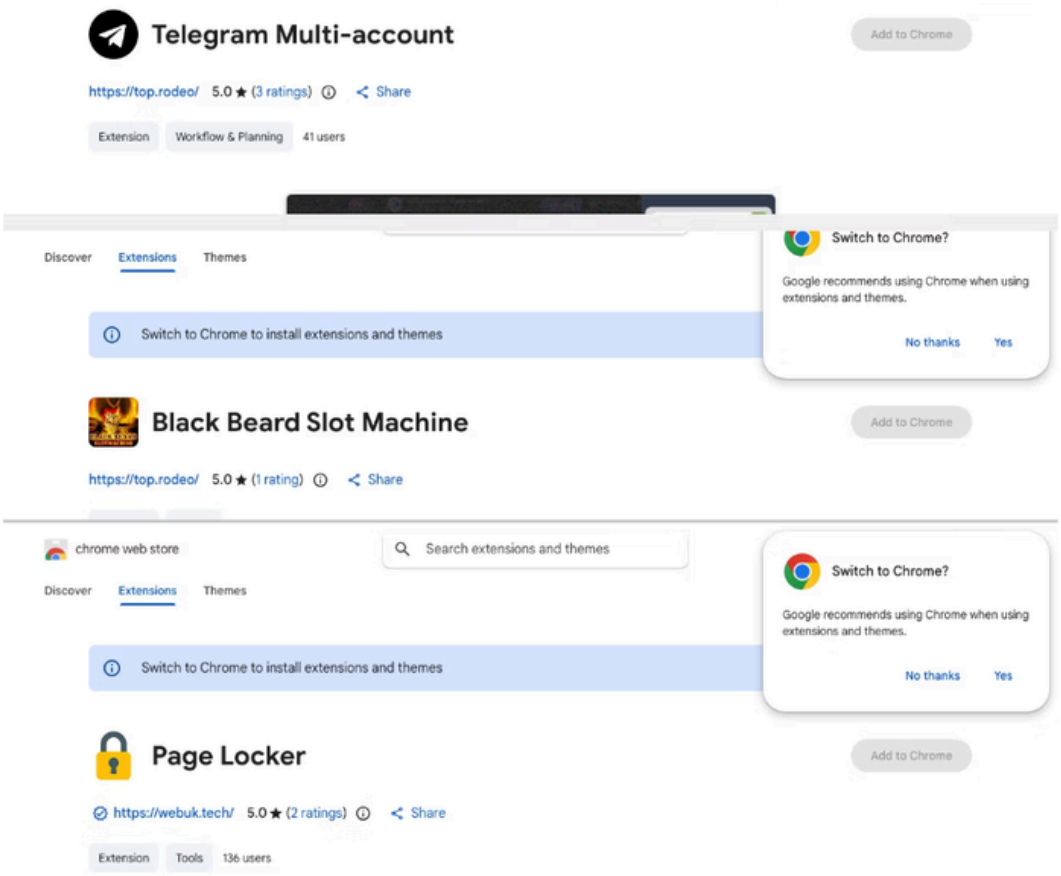
04 Riesgos emergentes en pagos digitales: malware NGate apunta a tecnología NFC en Android

05 Ciber Incidentes en Colombia y en el mundo

06 Contacto

01 108 extensiones maliciosas de Chrome roban datos de Google y Telegram

En un reciente hallazgo que pone en jaque la seguridad de miles de usuarios, investigadores de ciberseguridad han identificado una red de 108 extensiones maliciosas en la Chrome Web Store. Estas herramientas, diseñadas para parecer inofensivas, han logrado afectar a más de 20,000 personas, robando identidades de Google y sesiones de Telegram.



¿Cómo operan estas extensiones?

A pesar de ofrecer funciones desde utilidades para YouTube y TikTok hasta juegos de azar y clientes para Telegram todas comparten un mismo "cerebro": una infraestructura de comando y control (C2) única. Esto significa que, aunque parezcan aplicaciones distintas, todas envían la información robada al mismo servidor controlado por atacantes.

El peligro técnico oculto

El ataque es peligroso porque manipula la seguridad del navegador en tiempo real. Algunas extensiones usan la API declarativeNetRequest de Chrome para eliminar los encabezados de seguridad de los sitios web antes de la carga, dejando al usuario vulnerable a inyecciones de scripts maliciosos y anuncios fraudulentos.

¿Cómo protegerse?

Aunque Google ya ha sido notificado para retirar estas aplicaciones, es fundamental que los usuarios tomen medidas proactivas:

- **Auditoría inmediata:** Revisa tus extensiones instaladas (chrome://extensions/). Si no reconoces alguna o pertenece a los desarrolladores mencionados, elimínala de inmediato.
- **Principio de "Menos es Más":** Instala solo las extensiones estrictamente necesarias y de desarrolladores con reputación comprobada.
- **Vigila los permisos:** Sospecha de cualquier herramienta sencilla que solicite "leer y modificar todos los datos de los sitios web que visites".
- **Cierra sesiones:** Si sospechas que fuiste víctima, cierra todas las sesiones activas en tu cuenta de Google y Telegram, y cambia tus contraseñas de inmediato.

¡Conoce más aquí!

02 Expertos alertan: violación del **sistema de vigilancia del FBI es un incidente grave**

El FBI ha calificado como "incidente grave" la intrusión en su Red del Sistema de Recopilación Digital (DCSNet). Aunque no se vulneró el contenido de las comunicaciones, la filtración expuso metadatos estratégicos, información personal de sujetos investigados y detalles de operaciones de contrainteligencia bajo la ley FISA.

Aspectos importantes del Incidente:

Origen y Atribución: El ataque no fue directo, sino a través de una vulnerabilidad en la cadena de suministro (proveedores de internet). Se atribuye a hackers estatales chinos (Salt Typhoon), quienes ya habían comprometido a operadoras como AT&T y Verizon.

- Riesgo Estratégico: La filtración permite a potencias extranjeras identificar a quién vigila el FBI, qué métodos utiliza y qué investigaciones de contraterrorismo están activas.

- Fallas Sistémicas: Expertos señalan una deficiencia legislativa grave. Critican que leyes como CALEA exigen puertas de acceso para vigilancia gubernamental, pero no garantizan la seguridad de esa infraestructura frente a ciberataques de alto nivel.

Conclusión: El suceso resalta la fragilidad de la infraestructura crítica estadounidense y la falta de un marco normativo de seguridad de software comparable al de la Unión Europea, dejando al país vulnerable ante adversarios como China e Irán.

¡Conoce más aquí!

03 Adobe corrige activamente una vulnerabilidad de Acrobat Reader (CVE-2026-34621).

¿De qué se trata la vulnerabilidad?

Adobe ha publicado actualizaciones de seguridad de emergencia para corregir una vulnerabilidad crítica en Acrobat y Reader identificada como CVE-2026-34621, la cual está siendo explotada activamente en ataques reales. Esta falla, con una puntuación CVSS de 8.6, permite la ejecución de código arbitrario en los sistemas afectados, lo que representa un riesgo significativo para usuarios de Windows y macOS.

¿Cómo funciona el ataque?

La vulnerabilidad corresponde a un caso de prototype pollution, un tipo de fallo en JavaScript que permite a los atacantes manipular objetos internos de la aplicación. Mediante el uso de archivos PDF especialmente diseñados, los ciberdelincuentes pueden ejecutar código malicioso simplemente al abrir el documento, sin necesidad de interacción adicional, facilitando ataques dirigidos y campañas de phishing más efectivas.

¿Desde cuándo se está explotando?

Investigaciones indican que esta vulnerabilidad podría haber sido explotada desde diciembre de 2025, antes de que existiera un parche disponible, lo que aumenta su impacto.

Recomendaciones de seguridad

Ante este escenario, Adobe recomienda actualizar inmediatamente los productos afectados para mitigar riesgos, destacando la importancia de aplicar parches de seguridad de forma oportuna frente a amenazas activas en el entorno real.

¡Conoce más aquí!

04 Riesgos emergentes en pagos digitales: **malware NGate apunta a tecnología NFC en Android**

Una investigación de ESET Research revela una nueva variante del malware NGate que se oculta en una aplicación de pagos NFC aparentemente legítima en dispositivos Android. Esta amenaza utiliza una versión troyanizada de HandyPay para interceptar datos de tarjetas bancarias cuando el usuario configura el dispositivo como método de pago, permitiendo capturar información sensible como datos NFC y PIN sin generar sospechas.

La campaña activa desde finales de 2025 en Brasil utiliza ingeniería social a través de sitios y aplicaciones falsas. La información robada es enviada a los atacantes para cometer fraudes o retiros sin acceso físico a la tarjeta.

Recomendaciones

- Descargar aplicaciones solo de tiendas oficiales.
- Evitar instalar APKs de fuentes desconocidas.
- No conceder permisos innecesarios, especialmente en apps de pagos.
- No ingresar datos sensibles en aplicaciones no verificadas.
- Mantener el sistema operativo actualizado.

Vulnerabilidades **destacadas**

Microsoft SharePoint

CVE-2026-32201

Una validación de entrada incorrecta en Microsoft Office SharePoint permite que un atacante no autorizado realice suplantación de identidad a través de una red.

(RCE) en Windows

CVE-2026-33824

Double free en Windows IKE Extension permite que un atacante no autorizado ejecute código a través de una red.

Apache ActiveMQ

CVE-2026-34197

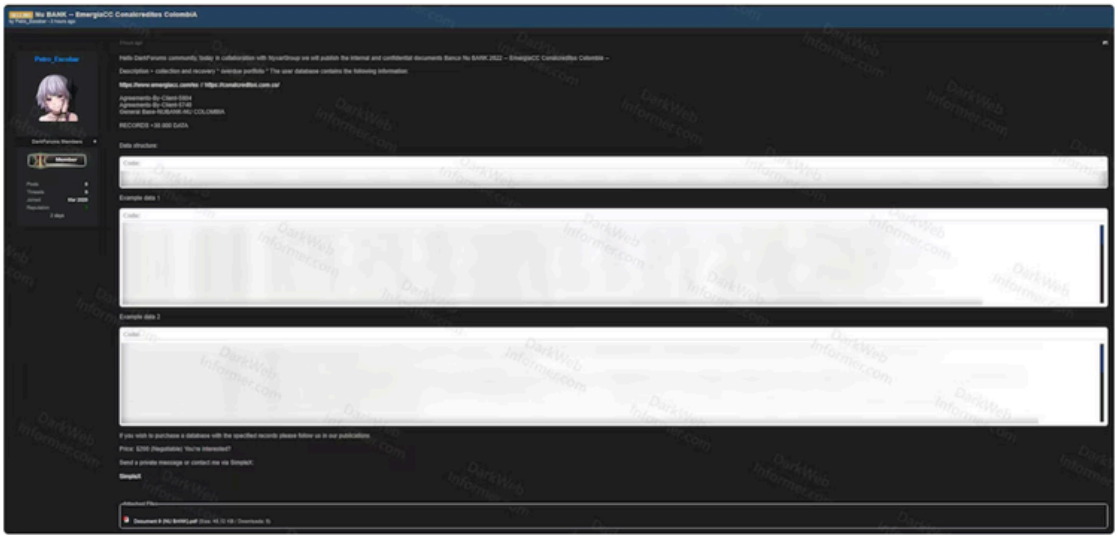
Vulnerabilidad de validación de entrada incorrecta, control incorrecto de generación de código ('inyección de código') en Apache ActiveMQ Broker, Apache ActiveMQ. Apache ActiveMQ Classic expone el puente JMX-HTTP Jolokia en /api/jolokia/ en la consola web.

¡Conoce más aquí!

05 Ciberincidentes en Colombia y en el mundo

Exposición de datos de clientes en Nubank Colombia por incidente en proveedor externo

Un incidente de ciberseguridad asociado a un proveedor externo de Nubank en Colombia expuso información de más de 30.000 clientes, la cual habría sido ofrecida en foros de la dark web. De acuerdo con el pronunciamiento oficial de la entidad, la brecha no se originó en sus sistemas, sino en una plataforma de terceros encargada de procesos de cobranza.



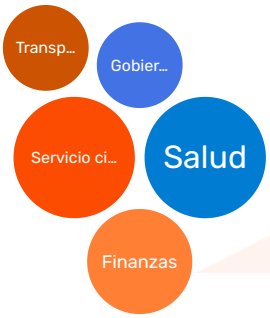
Los datos expuestos incluirían información sensible como nombres completos, números de identificación, teléfonos, estado de obligaciones financieras, montos adeudados y detalles de procesos de cobranza. Este nivel de detalle no solo permitiría identificar a las víctimas, sino también reconstruir su perfil financiero, facilitando posibles fraudes, extorsiones o suplantación de identidad.

Sin embargo, la entidad aclaró que el incidente no se originó en sus sistemas internos, sino en un proveedor externo encargado de la gestión de cobranzas. Nu Colombia indicó que no se comprometieron contraseñas ni productos financieros, y que se activaron protocolos de seguridad e investigaciones en conjunto con las autoridades para determinar el alcance real del evento.

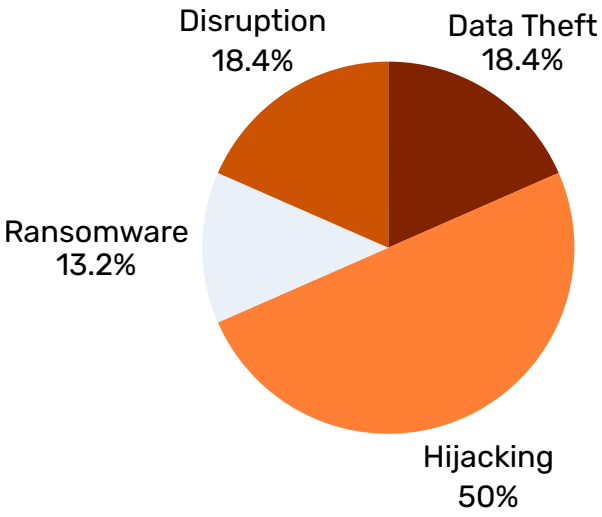
El mundo

20
Ciber incidentes

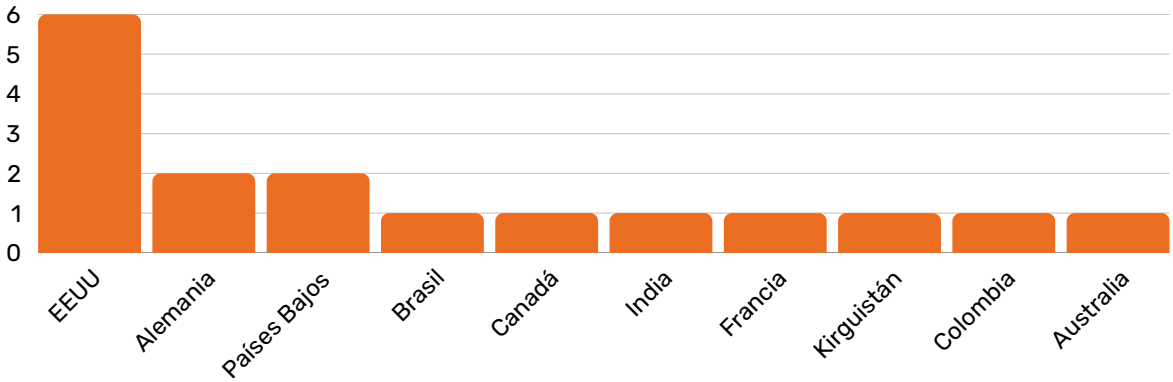
Sectores afectados



Tipo de incidente



Países destacados



¡Conoce más aquí!

E-dea Networks

Para información adicional sobre cualquiera de nuestros productos o servicios, por favor contáctanos:

Email: contacto@e-dea.co
Teléfono: (601) 57 1 5188433 opción 2
Celular: (601) 57 3152231023

Visita nuestro sitio para más información: www.e-dea.co
Encuéntranos en: Carrera 7 # 156-10 Of. 1906-1801.
Torre Krystal - Centro Empresarial North Point